RPO/RTO Impact on a
Disaster Recovery/Business Resumption Plan

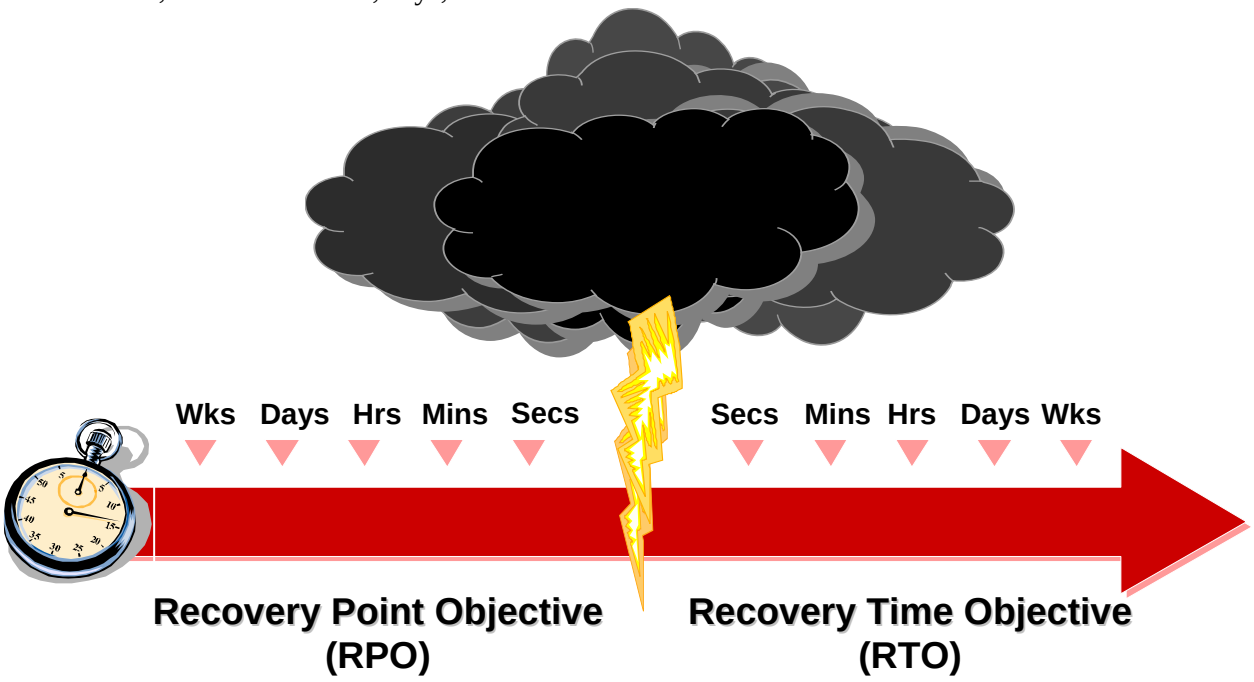
To date, in order to develop COOP plans, State entities have determined whether identified functions are Essential, Vital, Necessary, or Desired. That determination is based on the definitions found in the Process to assist ND State Entities in Developing a Continuum of Government Plan. Now it is time for the entities to take the next step – *identifying each business functions' Recovery Point Objective (RPO) and Recovery Time Objective (RTO).*

In the event of a disaster or audit, entities need to know when they can recover or locate their information. One of the first steps in this process is determining the data essential for the survival of your entity's business.

How Valuable Is Your Data?

Not all types of data are the same. Most of your organization's data is valuable. Some of it is *extremely valuable and/or absolutely critical to the survival of your entity's business* - **mission-critical** data. The following illustration helps understand the data status rating process.

Mission-critical data would have the shortest RPO. The shorter the RPO, the more current your backup data needs to be. The data that is classified as mission-critical requires up-to-the-minute data currency (the most current data available) to ensure that the recovery point is seconds or minutes, rather than hours, days, or even weeks.



The closer each number is to the disaster, the more expensive the budget cost will be. For example, if an essential function had an RPO of less than one hour, it would be necessary to have the information continually backed up so that the information is mirrored at an offsite. Naturally, there are IT costs associated with that type of recovery.

The key principle involved is that only those functions that must be performed because they are *key* to the survival of the organization should be listed as a top priority. The priorities of an agency may change as the duration of the service interruption lengthens. For example, a function that can sustain a delay of 3 days may become a top consideration if the interruption lasts a week.

How Much Can You Afford to Lose?

Determining the RPO/RTO formula for an identified function can be defined as:

> **Recovery Point Objective (RPO) –** In a disaster you will generally lose data. The *Recovery Point Objective* is the time (relative to the disaster) to which you could potentially recover your data. For example, if you make overnight backups, the recovery point objective could be the end of the previous day's activity.
>
> **Recovery Time Objective (RTO) –** This is the time period after a disaster at which a business function needs to be restored. Different business functions have different recovery time objectives. For example, the recovery time objective for the payroll function may be two weeks, whereas the recovery time objective for issuing a license may be two days.
>
> **Cost of downtime** — A state entity should calculate the potential losses it could incur, both as the result of a down time associated with the disaster and in recreating lost data.

Balancing the Tradeoffs

In an ideal world, organizations would develop backup processes that support up-to-the-minute currency for all their data. In the real world of limited resources, because of the costs involved, this approach just isn't feasible. Organizations must balance the tradeoff between currency of data and investment in resources. Getting this balance right is essential. Under-investing in data currency can result in the collapse of the entity in the event of a disaster. Over-investing in protecting non-critical data can tie up valuable resources better used elsewhere in your disaster recovery and Continuity of Operations programs.

Continuous Backup Maximizes Data Currency

Once you have classified your organization's data according to Recovery Time and Recovery Point Objectives, State entities will need to work with ITD to develop and implement appropriate backup technologies and processes accordingly. For the most critical data with the shortest RPO, a solution such as electronic vaulting that supports continuous backup will need to be implemented. Unlike periodic backup processes that ensure recovery of data only up to the point that the backup was done, continuous backup closes the window for potentially lost data. While you can never absolutely guarantee zero loss of data, continuous backup solutions can minimize data loss to minutes or even seconds.

Data recovery budget —

The following criteria can assist in determining the criticality of business functions. There may be others that are of importance to an agency.

- Maintenance of public health and safety.

- Income maintenance for citizens.
- Income maintenance for government employees.
- Payments to vendors for goods and services.
- Requirements for compliance or regulation.
- Effect on state government cash flow.
- Criticality Classification.
- Effect on production and delivery of services.
- Volume of activity and recovery costs.
- Effect on public image.
- Inter-system dependency.

The following categorization is suggested as a means for classifying computer application systems used by an agency:

- Must be processed in normal mode; no degradation is acceptable.
- Only high priority; e.g., high dollar item transactions or critical reports will be processed.
- Processing will be carried out on a "time available" only basis.
- Processing will be suspended, but data collection will continue.
- No processing or data collection will be carried out until normal computer capacity is reestablished.

Conclusion

State entities carry out hundreds of operations that management and staff consider important. Key resources may be unavailable during a disaster. *The entity must concentrate its resources on those operations that are most important for public health, safety, and welfare*. The aim of a disaster recovery/business resumption plan is to reduce potential losses, not to duplicate a business-as-usual environment.